The Incident Reporting Tool User Guide

This guide provides an overview of how to access and use the IG Toolkit Incident Reporting Tool.

Please note that the screen shots in this guide are taken from our test site which is indicated by the yellow bar at the top of each screen shot. In the production application users will see the pages in the sections 1 to 4 without the yellow banding at the top of the page.

To make the guide easier to follow it has been split into four main sections:

---

1. About the Incident Reporting Tool

A. Incident Reporting Tool Overview?

The Incident Reporting Tool is an online tool hosted on the secure Information Governance Toolkit website.

- It is the Department of Health (DH) and Information Commissioner's Office (ICO) agreed mechanism for Health and Social Care organisations' to report data breach incidents.

- It is the Department of Health (DH) and National Cyber Security Programme[1] sponsored reporting mechanism providing Health and Social Care sector a facility to report Cyber Security Serious Incidents Requiring Investigation (Cyber SIRI).

- Accessible by all organisations' registered with the IG Toolkit website when permissions are granted.

[1] The NCSP is managed and coordinated on behalf of Government by the Office of Cyber Security and Information Assurance in the Cabinet Office, under the oversight of the Minister for the Cabinet Office. - https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

- All Organisation Administrators are automatically given permissions to access the Incident Reporting section of the IG Toolkit but they can withdraw access if not required. Organisation Administrators can also grant permissions for additional Incident Reporting Users via their Organisation Admin section.

- Organisations can only see incidents recorded against their organisation code. They cannot view other incidents until information is published on the IG Toolkit website.

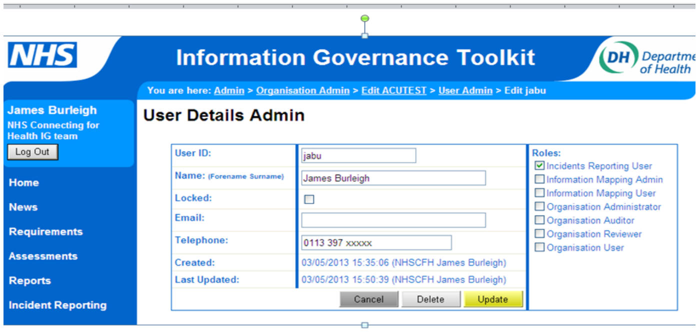
- The Incident Reporting Tool provides features and functionality such as:
  - Adding a new incident
  - Updating existing records of incidents
  - Notifying a Level 2 SIRI now or save to notify later
  - Recording authorisation to report a SIRI e.g. a note of approver's name and role such as the SIRO or Caldicott Guardian. This can be marked as 'Not required' if the person providing the notification has been given the authorisation already by the SIRO or other approver.
  - Marking incidents as duplicates or withdrawn if added in error
  - Exporting details of individual incidents into a Word document.
  - Date range reports to allow for quarterly, all time or specific date range reports. These can be viewed online or exported to Word or Excel
  - Automated notification emails to the national bodies e.g. DH, HSCIC, and ICO as appropriate.

- Further information on the requirement to report, manage and investigate Incidents can be found on the Incident Reporting Tool landing page called 'Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation' (this document is found in the 'Publications' section on the home page).

B. How to access the Incident Reporting Tool

All IG Toolkit Organisation Administrators for all organisation types are automatically assigned Incident Reporting user permissions. . They can choose to opt out and they can grant permissions to other users to have access to the Incident reporting rights. Once these permissions have been granted the user will see the 'Incident Reporting' tab on the left side menu when logged into the IG Toolkit home page. Other members of the organisation who require access to this tool should contact their local IG Toolkit Organisation Administrator. The steps an Organisation Administrator need to take to grant Incident Reporting permissions to other users are :-

1. **Login to the IG Toolkit.**
2. **Click on the 'Admin' tab on the left side menu**
3. **Select the 'User Admin' option**
4. **Then either click on 'edit' against the relevant existing user's account, or click on 'Add New User'.**
5. **User access can be granted by ticking the 'Incidents Reporting User' tick box, and for new users you will also need to complete the name, email and telephone details which are then e-mailed to the user with the login ID and password.**



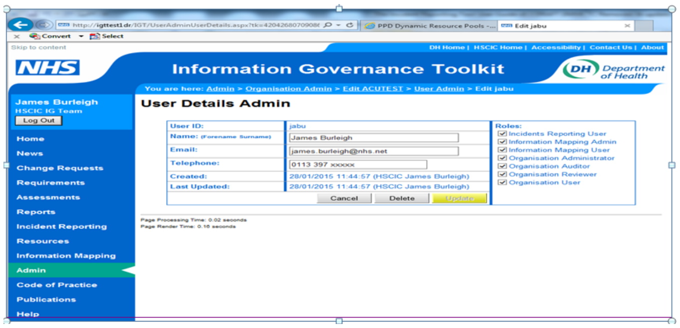
You are here: Admin > Organisation Admin > Edit ACUTEST > User Admin > Edit jabu

User Details Admin

User ID:	jabu
Name: (Forename Surname)	James Burleigh
Locked:	□
Email:	
Telephone:	0113 397 xxxxx
Created:	03/05/2013 15:35:06 (NHSCFH James Burleigh)
Last Updated:	03/05/2013 15:50:39 (NHSCFH James Burleigh)

Roles:
☑ Incidents Reporting User
□ Information Mapping Admin
□ Information Mapping User
□ Organisation Administrator
□ Organisation Auditor
□ Organisation Reviewer
□ Organisation User

6. If a new user is enrolled as an Organisation Administrator then the Incidents Reporting User tab will be automatically ticked which will give them access to record incidents- unless the user opts out of Incident Reporting permissions by un-ticking the tab.



You are here: Admin > Organisation Admin > Edit ACUTEST > User Admin > Edit jabu

User Details Admin

User ID:	jabu
Name: (Forename Surname)	James Burleigh
Email:	james.burleigh@nhs.net
Telephone:	0113 397 xxxxx
Created:	28/01/2015 11:44:57 (HSCIC James Burleigh)
Last Updated:	28/01/2015 11:44:57 (HSCIC James Burleigh)

Roles:
☑ Incidents Reporting User
☑ Information Mapping Admin
☑ Information Mapping User
☑ Organisation Administrator
☑ Organisation Auditor
☑ Organisation Reviewer
☑ Organisation User

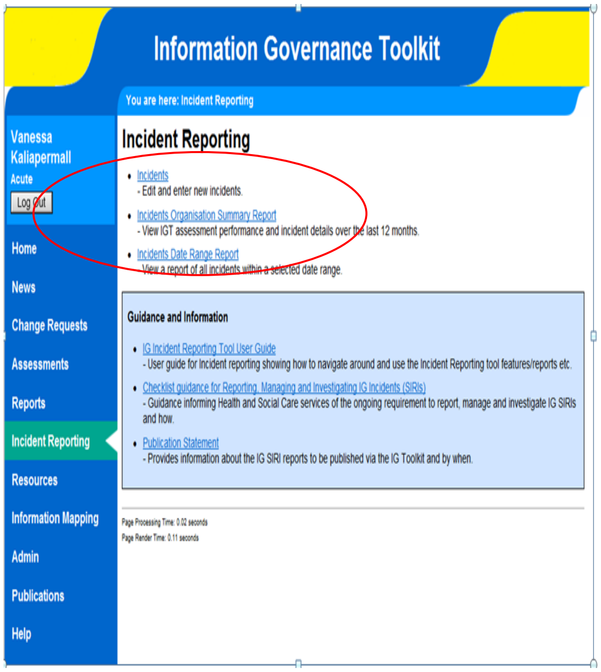
Page Processing Time: 0.02 seconds
Page Render Time: 0.16 seconds

7. All Organisation Administrators are automatically assigned Incident Reporting user rights unless they decide to opt out.

8. The Organisation Administrator will need to repeat the process for adding a new Incident Reporting User above for each user that they want to grant access to the Incident Reporting Tool.

C. The Incident Reporting Tool landing page

There are 3 areas available to Incident Reporting Tool Users and supporting guidance/information. See screen shot below.



You are here: Incident Reporting

Incident Reporting

- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

- IG Incident Reporting Tool User Guide
  - User guide for Incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

Incidents – this allows users to create a new, search, edit or close an existing incident record. Organisations can view a total number of Incidents recorded, export a full list of incidents into Excel, extract individual reports of each incident, export individual incidents into Word and sort the columns of the searched data as preferred.

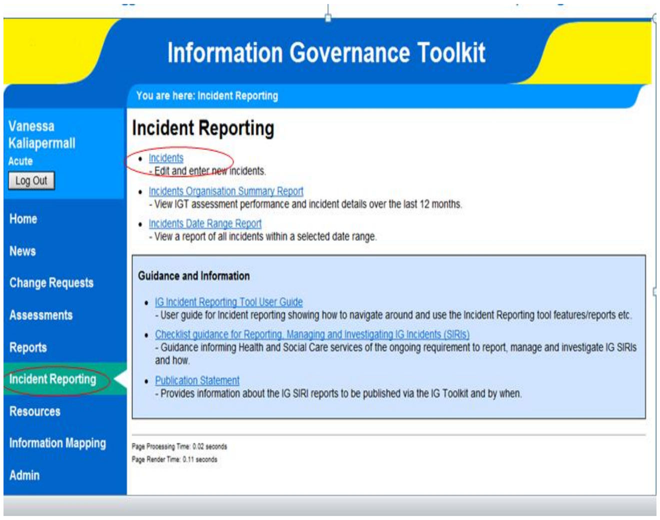
Incident Organisation Summary Report – presents a report on IG or Cyber SIRIs, (exportable in Word format) which could be used to inform senior management, Boards or interested Committees of any incidents which have been recorded in the last 12 months and an overview of the organisation's latest published IG Toolkit performance. This report also displays the latest recorded senior management details entered by (in most cases) the Organisation Administrator via the IG Toolkit Assessment Summary Screen.

Incident Date Range Report – This area allows Incident Reporting Tool Users to run summary reports of all IG or Cyber Security related Incidents within a selected quarter or date range and export data into Excel or Word.

2 How to Create, Update or Close an Incident

A. How to create and complete a new Incident
B. Updating or editing an existing incident
C. Closing an incident
D. Re-opening an incident

A. How to create and complete a new Incident



You are here: Incident Reporting

Incident Reporting

- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

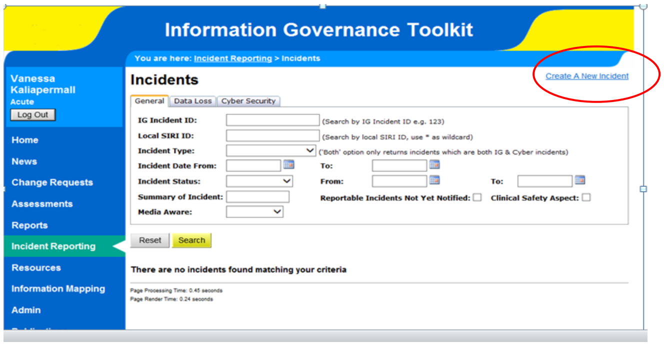
- IG Incident Reporting Tool User Guide
  - User guide for Incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

1. When logged in click on the 'Incidents' Link found on the 'Incident Reporting' left side menu tab.

2. A list of any recorded Incidents will appear on the screen with an option to export to Excel or click through to edit an existing Incident record and the total number of incidents recorded for your Organisation on this Tool to date. If there are no incidents reported then this screen will be blank with a link to 'Create a new incident' only.

3. To input a new incident click the 'Create a New Incident' link (top right of the screen).



You are here: Incident Reporting > Incidents

Incidents

IG Incident ID: (Search by IG Incident ID e.g. 123)
Local SIRI ID: (Search by local SIRI ID, use * as wildcard)
Incident Type: ('Both' option only returns incidents which are both IG & Cyber incidents)
Incident Date From: To:
Incident Status: From: To:
Summary of Incident: Reportable Incidents Not Yet Notified: □ Clinical Safety Aspect: □
Media Aware:

There are no incidents found matching your criteria

Page Processing Time: 0.45 seconds
Page Render Time: 0.24 seconds

<u>Please note: If the organisation has no incidents listed then this screen will be blank. ***</u>***

4. After clicking on 'Create a new Incident' the Incident details screen will appear. User must select the appropriate incident type e.g. Cyber SIRI, IG SIRI or if applicable you can tick both boxes. You should also ensure that you read the disclaimer at the top of the screen in red text. See example of text below.

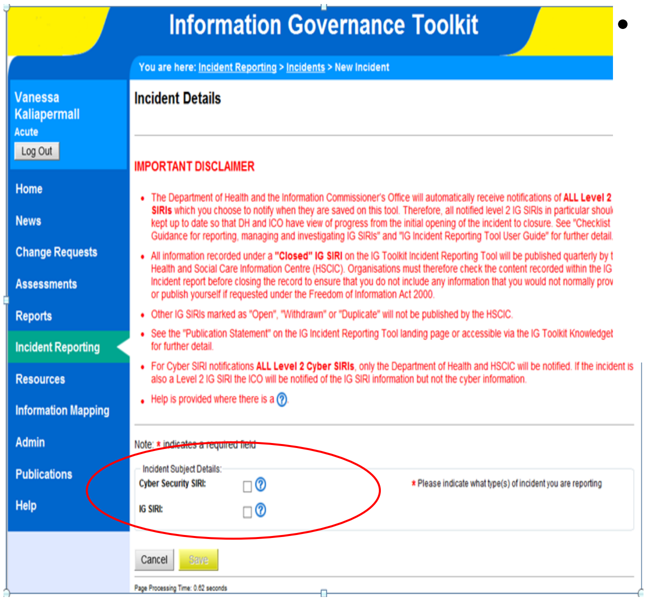
***IMPORTANT DISCLAIMER**

- The Department of Health and the Information Commissioner's Office will automatically receive notifications of **ALL Level 2 IG SIRIs** which have been recorded and saved on this tool. Therefore, all notified level 2 IG SIRIs in particular should be kept up to date so that DH and ICO have view of progress from the initial opening of the incident to closure. See "Checklist Guidance for Reporting, Managing and Investigating IG and Cyber SIRIs" and "The Incident Reporting Tool User Guide" for further detail.

- Ensure that the incident is closed as soon as practicable or appropriate. We would not expect the incident to be in 'Open' status for more than 3 months usually.

- All information recorded under a **"Closed" IG SIRI** record on the Incident Reporting Tool will be published quarterly by the Health and Social Care Information Centre (HSCIC). Organisations must therefore check the content recorded within the IG Incident report before closing the record to ensure that you do not include any information that you would not normally provide or publish yourself if requested under the Freedom of Information Act 2000. Ensure the record is up to date, factual and accurate in content e.g. check spelling, grammar, no person identifiable data etc. Content should be appropriate for publication.

- Cyber information and SIRIs marked as ‘Level 2 TBC’, "Open", "Withdrawn" or "Duplicate" will not be published by the HSCIC.
- See the "Publication Statement" on the Incident Reporting Tool landing page and accessible via the IG Toolkit Knowledgebase or Publications sections for further detail on our routine publications, what information we share, with whom and for what purpose.
- Only the Department of Health and HSCIC will receive notifications of **ALL Level 2 Cyber SIRIs.** If the Cyber incident is also classed as a Level 2 IG SIRI the ICO will be notified of the IG SIRI information but not the cyber information entered.
- Further Help on the data entry fields is provided where there is a ? symbol.



You are here: Incident Reporting > Incidents > New Incident

Incident Details

IMPORTANT DISCLAIMER

- The Department of Health and the Information Commissioner's Office will automatically receive notifications of **ALL Level 2 SIRIs** which you choose to notify when they are saved on this tool. Therefore, all notified level 2 IG SIRIs in particular shoul kept up to date so that DH and ICO have view of progress from the initial opening of the incident to closure. See "Checklist Guidance for reporting, managing and investigating IG SIRIs" and "IG Incident Reporting Tool User Guide" for further detail.
- All information recorded under a **"Closed" IG SIRI** on the IG Toolkit Incident Reporting Tool will be published quarterly by t Health and Social Care Information Centre (HSCIC). Organisations must therefore check the content recorded within the IG Incident report before closing the record to ensure that you do not include any information that you would not normally prov or publish yourself if requested under the Freedom of Information Act 2000.
- Other IG SIRIs marked as "Open", "Withdrawn" or "Duplicate" will not be published by the HSCIC.
- See the "Publication Statement" on the IG Incident Reporting Tool landing page or accessible via the IG Toolkit Knowledget for further detail.
- For Cyber SIRI notifications **ALL Level 2 Cyber SIRIs**, only the Department of Health and HSCIC will be notified. If the incident is also a Level 2 IG SIRI the ICO will be notified of the IG SIRI information but not the cyber information.
- Help is provided where there is a ?.

Note: * indicates a required field

Incident Subject Details:

Cyber Security SIRI: □ ?

IG SIRI: □ ?

* Please indicate what type(s) of incident you are reporting

Page Processing Time: 0.62 seconds

5. The type of incident selected will determine the appropriate incident reporting form. You will see the screen populate with the relevant data entry fields as you select an option. For further details on which data fields apply for Cyber SIRIs or IG SIRIs see Annex A . Where both are selected then all the data fields appear on the screen. The data fields on this incident input screen contain dropdown lists to select from mainly, some system generated fields and minimal free text fields for capturing more detailed information.

**Please note: Users are strongly advised to click on and read the context help ? symbols where displayed against certain data fields. There is some useful information behind these, defining categories, warning regarding information recorded under certain free text fields and guidance on the type of information to be included under the data field.********

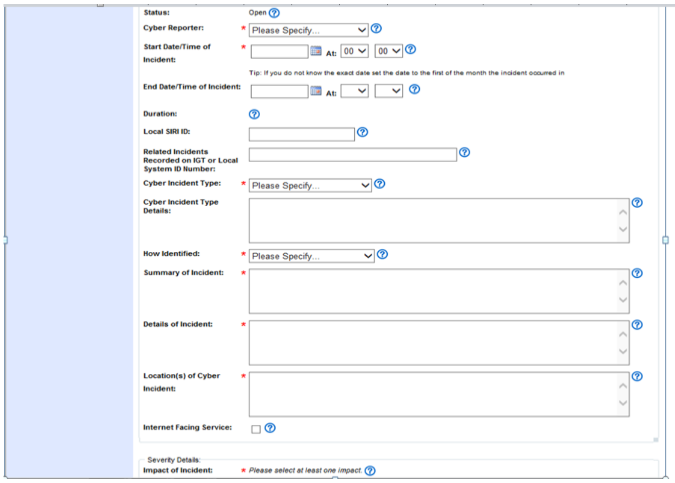
6. There are a total of 7 sections to complete in the incident report form:-

- **Incident Subject Details**
- **General Details**
- **Severity Details**
- **Data Details**
- **Post Incident Details**
- **Information Commissioner's Office (ICO) Information**

- Authorisation (Only appears for incidents which meet Level 2 severity)

<u>Please note: The data fields which are marked with an asterix * are mandatory fields which means they must be populated before the form can be saved or notified. ***</u>***

The screen looks like this:-



Status:		Open ?
Cyber Reporter:	*	Please Specify... ?
Start Date/Time of Incident:	*	At: 00 00 ?
		Tip: If you do not know the exact date set the date to the first of the month the incident occurred in
End Date/Time of Incident:		At: ?
Duration:		?
Local SIRI ID:		?
Related Incidents Recorded on IGT or Local System ID Number:		?
Cyber Incident Type:	*	Please Specify... ?
Cyber Incident Type Details:		?
How Identified:	*	Please Specify... ?
Summary of Incident:	*	?
Details of Incident:	*	?
Location(s) of Cyber Incident:	*	?
Internet Facing Service:		□ ?

Severity Details:

Impact of Incident:	*	*Please select at least one impact.* ?

7. After each field has been considered and populated the user can elect to notify a level 2 incident by clicking on the 'Notify Now' or 'Notify Later' options and then clicking on the 'save' button. Incidents which are of a lower severity do not view the 'Authorisation' section; it is only relevant to Level 2 incidents. If the user chooses to 'Notify Now' an incident warning message will appear at this stage to inform the user that saving this incident will result in an email being sent to the relevant interested parties e.g. DH, ICO, HSCIC (as appropriate).

*****Please note: IG Level 2 SIRIs are sent to the HSCIC, NHS England, DH and the ICO. Cyber Level 2 SIRIs are only sent to HSCIC and the DH. *****

8. If the incident has been assessed at severity Level 2 in error the user will be given the opportunity to return to the incident record and amend the incident as necessary e.g. downgrade or mark as withdrawn or duplicate. This will trigger another email to the notification recipients informing them that the incident is no longer classed as Level 2 SIRI.

9. Therefore, the system allows a user to choose whether to 1) save and report the level 2 incident immediately by ticking the 'Notify Now' box (see 5 above) or 2) you can save the Level 2 incident to 'Notify Later'. This would allow users time to forward the incident to senior responsible managers e.g. the Caldicott Guardian or SIRO and seek authorisation to approve notification of the incident to the relevant DH and HSCIC. Once 'Notify Later' is ticked the 'message from webpage' will display and say that the incident will be saved on the incident system but will not be notified to regulators. The message is slightly different for IG and Cyber incidents. The message will keep displaying each time you save an update to the record and until you mark the incident for notification or change the severity level.

10. The incident must not be left in Level 2 (TBC) e.g. Notify later status for a long period. Ensure you report in accordance with the HSCIC guidance supporting the use of the Incident reporting Tool.

11. The user may forward the incident for authorisation that an approver agrees that it is a level 2 notifiable incident. Once the approver agrees that it's a level 2 notifiable incident the user may mark the incident 'Approved field' as appropriate e.g. Yes, No or Not Required. Complete the Approver Name and Approver Role fields and then save the incident after selecting 'Notify now'. It is a local organisation decision to seek authorisation or not. This is not mandatory as organisations devolve responsibilities in a variety of ways but it was upon request of users that this function would be very helpful whilst they assess the severity of the incident, discuss with senior colleagues and then decide

to notify. This is probably more significant when there is a Level 2 IG SIRI which when confirmed is required to be notified to the formal regulator for Data Breaches of the Data Protection Act, the ICO.

12. **Timelines for level 2 ‘pending approval’ are as described in the latest SIRI Checklist guidance which can be found on the IG Toolkit home page under ‘Publications’ and users should make every effort to report the level 2 incident in line with this guidance.**

Please note: the tool is set up to ensure maximum information is provided therefore the incident cannot be saved unless all the mandatory fields are populated. A warning message (at the top of the screen in red text) will offer guidance where mandatory fields may not have been populated. If certain information is unknown then use the ‘Not known’ categories where available or select the option which best represents the current position. As soon as information is known please update the record. ***

INFORMATION BOX

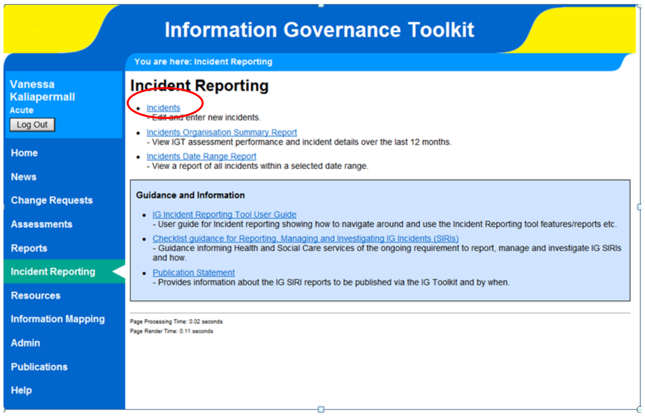
- **The completion of the online reporting form should be quite straight forward and should not take much time to complete.**

- **Additional useful guidance on Breach Types (definitions and examples) and assessment of the incident severity can be found within the ‘Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (IG SIRI) (including Cyber SIRI Incidents)’ Annexes found on the Incident Reporting Tool landing page.**

B. Updating or editing an existing incident.

To update or edit an incident the user needs to follow the process below

1. **Click on the ‘Incidents’ Link**



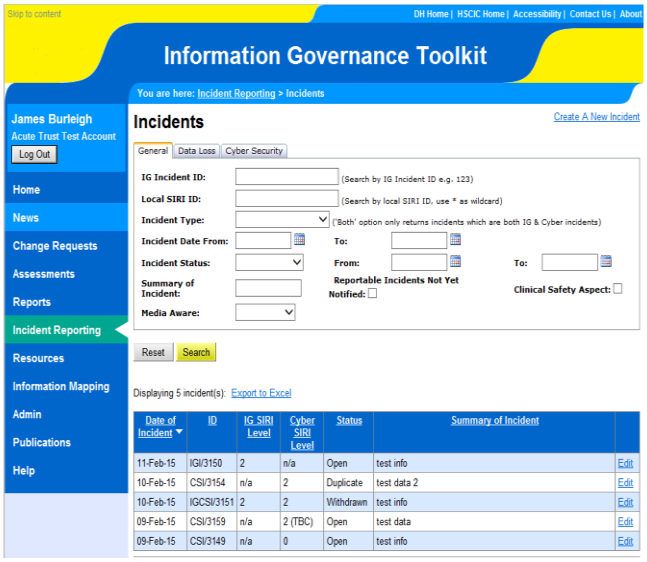
Incident Reporting

- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

- IG Incident Reporting Tool User Guide
  - User guide for Incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds



You are here: Incident Reporting > Incidents

Incidents

Create A New Incident

General | Data Loss | Cyber Security

IG Incident ID: (Search by IG Incident ID e.g. 123)

Local SIRI ID: (Search by local SIRI ID, use * as wildcard)

Incident Type: ('Both' option only returns incidents which are both IG & Cyber incidents)

Incident Date From: To:

Incident Status: From: To:

Summary of Incident: Reportable Incidents Not Yet Notified: □ Clinical Safety Aspect: □

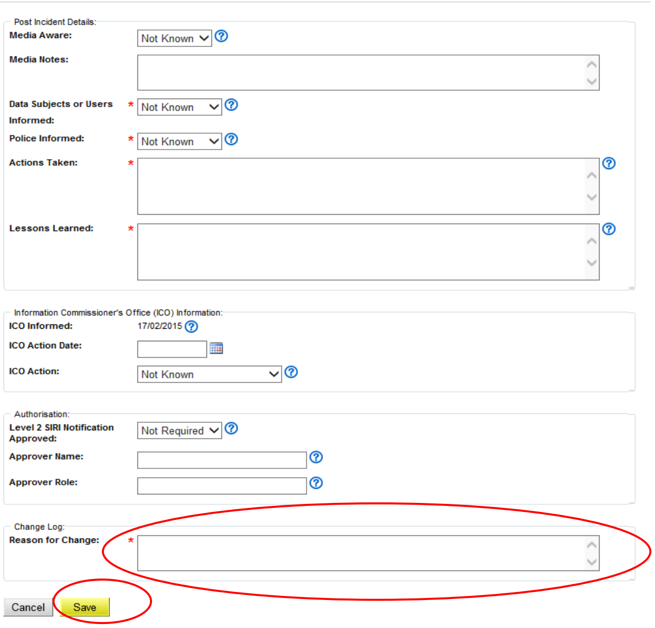
Media Aware:

Reset | Search

Displaying 5 incident(s): Export to Excel

Date of Incident ▼	ID	IG SIRI Level	Cyber SIRI Level	Status	Summary of Incident	
11-Feb-15	IGI/3150	2	n/a	Open	test info	Edit
10-Feb-15	CSI/3154	n/a	2	Duplicate	test data 2	Edit
10-Feb-15	IGCSI/3151	2	2	Withdrawn	test info	Edit
09-Feb-15	CSI/3159	n/a	2 (TBC)	Open	test data	Edit
09-Feb-15	CSI/3149	n/a	0	Open	test info	Edit

2.Navigate to the relevant incident either from this list on the screen or by using the General, Data Loss or Cyber Security search tabs facility and click on 'edit' against the incident you wish to update



Post Incident Details:

Media Aware:	Not Known
Media Notes:	
Data Subjects or Users Informed: *	Not Known
Police Informed: *	Not Known
Actions Taken: *	
Lessons Learned: *	

Information Commissioner's Office (ICO) Information:

ICO Informed:	17/02/2015
ICO Action Date:	
ICO Action:	Not Known

Authorisation:

Level 2 SIRI Notification Approved:	Not Required
Approver Name:	
Approver Role:	

Change Log:

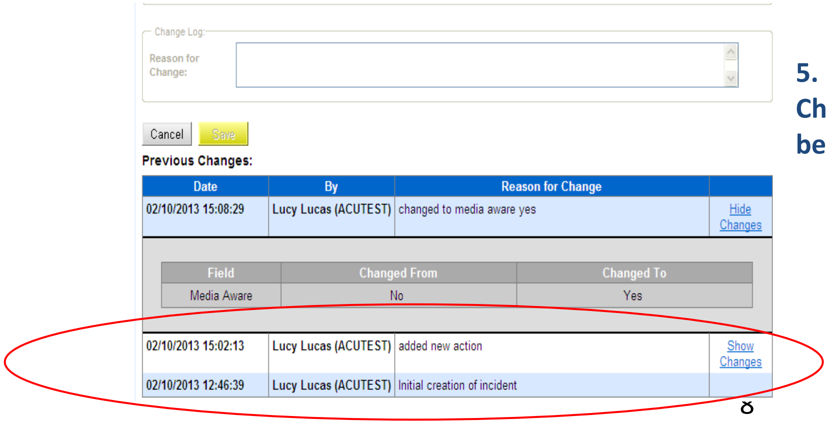
Reason for Change: *

Cancel | Save

3. You will be taken to the incident details page. Update the relevant field(s) e.g. if you change the Status field from Open to Closed and enter a reason for the change in the 'reason for change' field at the bottom of the page.

4. Click the 'save' button and the page will refresh. Your updates will then be saved and will also appear in the 'previous changes' log at the bottom of the page.

_ Please note that where the SIRI level changes to a 2 after an update has been completed then the Authorisation section will appear and you can decide to notify now or later.***_***



Change Log:

Reason for Change:

Cancel | Save

Previous Changes:

Date	By	Reason for Change	
02/10/2013 15:08:29	Lucy Lucas (ACUTEST)	changed to media aware yes	Hide Changes

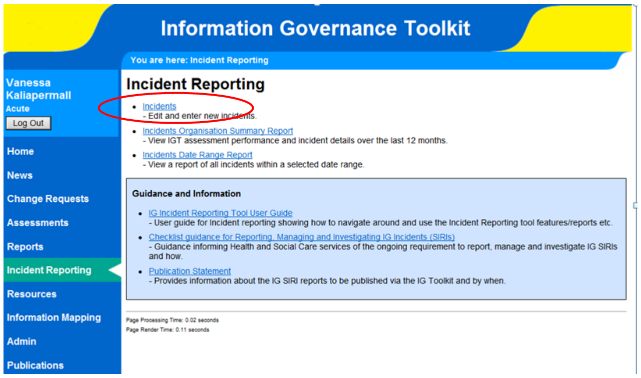
Field	Changed From	Changed To
Media Aware	No	Yes

Date	By	Reason for Change	
02/10/2013 15:02:13	Lucy Lucas (ACUTEST)	added new action	Show Changes
02/10/2013 12:46:39	Lucy Lucas (ACUTEST)	Initial creation of incident	

5. For audit and or review purposes the 'Show Changes' link will provide an audit trail of what has been changed, when and by whom, as shown below.

C. Closing an incident

1. Click on the 'Incidents' Link



Incident Reporting

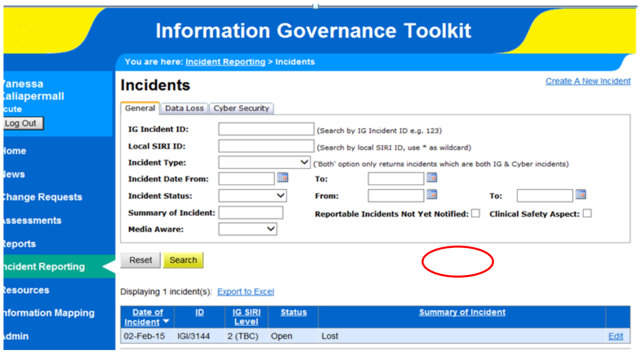
- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

- IG Incident Reporting Tool User Guide
  - User guide for Incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

2. Navigate to the relevant Incident either from this list on the screen or by using the basic or advanced search facility and click on 'edit' against the incident you wish to close.



Incidents

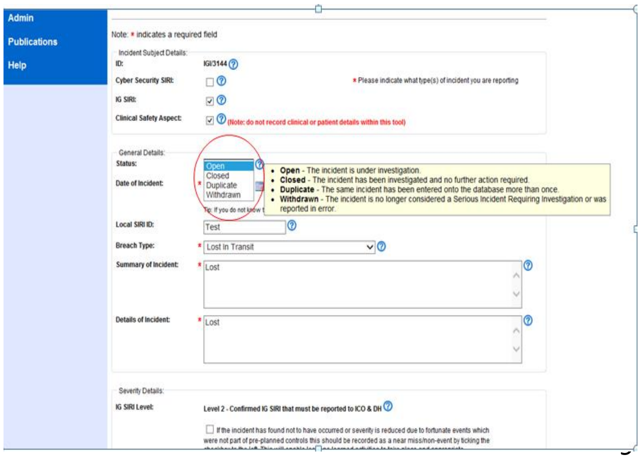
IG Incident ID: (Search by IG Incident ID e.g. 123)
Local SIRI ID: (Search by local SIRI ID, use * as wildcard)
Incident Type: ('Both' option only returns incidents which are both IG & Cyber incidents)
Incident Date From: To:
Incident Status: From: To:
Summary of Incident: Reportable Incidents Not Yet Notified: □ Clinical Safety Aspect: □
Media Aware:

Displaying 1 incident(s): Export to Excel

Date of Incident ▼	ID	IG SIRI Level	Status	Summary of Incident	
02-Feb-15	IGI/3144	2 (TBC)	Open	Lost	Edit

3. Update the 'status' field as shown below to 'Closed' and ensure all the fields under 'Post Incident Details' section, 'Information Commissioner's Office Information' section and the 'Local SIRI ID' field are populated with the latest position. Click the 'save' button to save the change of status.

Please note: The 'lessons learned' and 'Actions taken' fields are particularly important upon closure of an incident so that we can learn from experience and identify gaps or requirements for further guidance to support the improvements to performance regarding incidents and hopefully work proactively to prevent incidents from reoccurring. Once an incident has been closed the lessons learned and actions taken fields can still be updated to accurately reflect any additional lessons / actions implemented since the incident was closed. These incidents will be included within reports published on the IG Toolkit 'Publications' page so ensure that the information is accurate (including grammar and spelling) and does not include anything which you would not disclose under the Freedom of Information Act 2000



Note: * indicates a required field

Incident Subject Details:
ID: IGI/3144
Cyber Security SIRI: □ * Please indicate what type(s) of incident you are reporting
IG SIRI: ☑
Clinical Safety Aspect: ☑ (Note: do not record clinical or patient details within this tool)

General Details:
Status: Open / Closed / Duplicate / Withdrawn

- **Open** - The incident is under investigation.
- **Closed** - The incident has been investigated and no further action required.
- **Duplicate** - The same incident has been entered onto the database more than once.
- **Withdrawn** - The incident is no longer considered a Serious Incident Requiring Investigation or was reported in error.

Date of Incident: *
Tip: If you do not know t
Local SIRI ID: Test
Breach Type: * Lost In Transit
Summary of Incident: * Lost
Details of Incident: * Lost

Severity Details:
IG SIRI Level: Level 2 - Confirmed IG SIRI that must be reported to ICO & DH

□ If the incident has found not to have occurred or severity is reduced due to fortunate events which were not part of pre-planned controls this should be recorded as a near miss/non-event by ticking the

4. Click the 'save' button and the page will refresh. The updates will then be saved and will appear in the 'previous changes' log at the bottom of the page, as described above under 'Updating or editing an existing incident'.

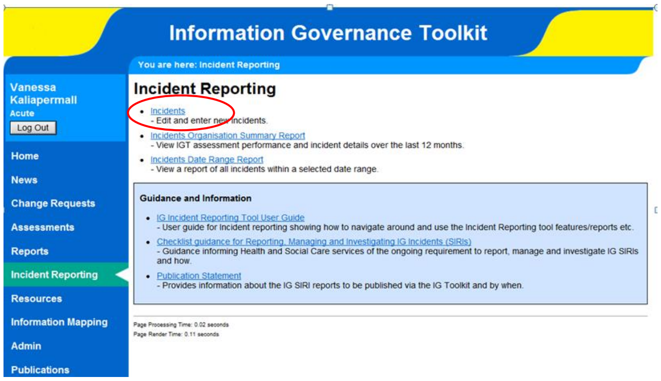
***Please note that this screen and content recorded within it can be exported to Word and saved as an attachment to escalate incidents to internal senior

management, IG Lead, Senior Information Risk Owner (SIRO), Caldicott Guardian etc, as required.***

Note that the release of IG Toolkit v.13 will introduce an 'auto closure' feature whereby incidents where no updates to an 'open' record have been undertaken within the last 90 days will be closed. Relevant incident reporting users will be notified by email 10 days in advance of planned auto closure and within 24 hours after closure. Further details are described in Appendix A of the 'Incident Reporting Tool User Guide'. Note that autoclosed incidents can be re-opened as per section D below.

D. Re-opening an incident

1. Click on the 'Incidents' Link



Information Governance Toolkit

You are here: Incident Reporting

Vanessa Kaliapermall
Acute

Incident Reporting

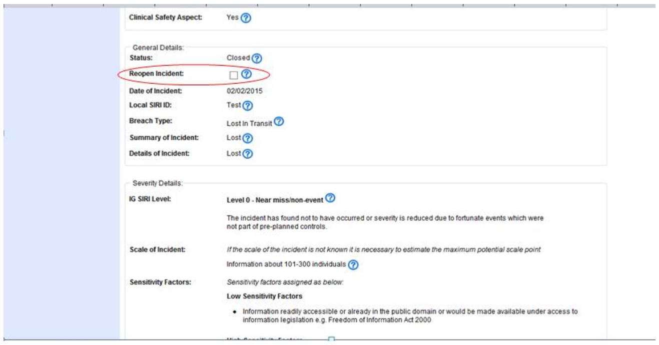
- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

- IG Incident Reporting Tool User Guide
  - User guide for Incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

2. Navigate to the relevant incident either from this list on the screen or by using the basic or advanced search facility and click on 'edit' against the incident you wish to re-open.



Clinical Safety Aspect:	Yes

General Details:

Status:	Closed
Reopen Incident:	□
Date of Incident:	02/02/2015
Local SIRI ID:	Test
Breach Type:	Lost In Transit
Summary of Incident:	Lost
Details of Incident:	Lost

Severity Details:

IG SIRI Level: Level 0 - Near miss/non-event

The incident has found not to have occurred or severity is reduced due to fortunate events which were not part of pre-planned controls.

Scale of Incident: *If the scale of the incident is not known it is necessary to estimate the maximum potential scale point*

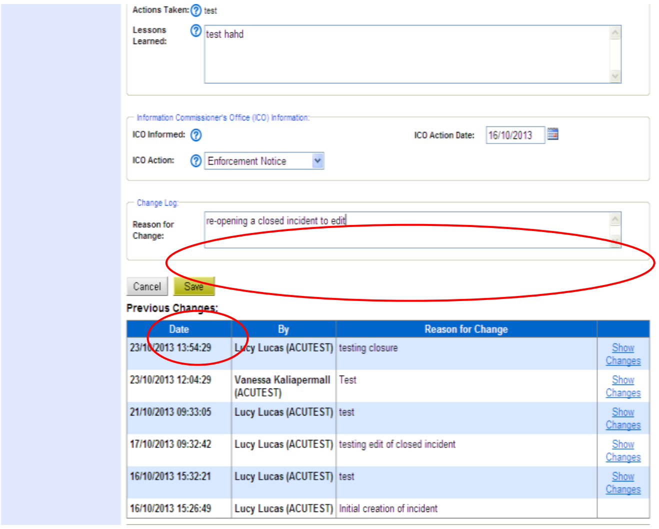
Information about 101-300 individuals

Sensitivity Factors: *Sensitivity factors assigned as below:*

Low Sensitivity Factors

- Information readily accessible or already in the public domain or would be made available under access to information legislation e.g. Freedom of Information Act 2000

3. Check the 'Reopen Incident' box, and enter details on the reason for change in the field at the bottom of the page, then click the 'save' button towards the bottom of the screen to reopen the incident as demonstrated in the two screenshots below.



Actions Taken: test

Lessons Learned: test hahd

Information Commissioner's Office (ICO) Information:

ICO Informed:

ICO Action Date: 16/10/2013

ICO Action: Enforcement Notice

Change Log:

Reason for Change: re-opening a closed incident to edit

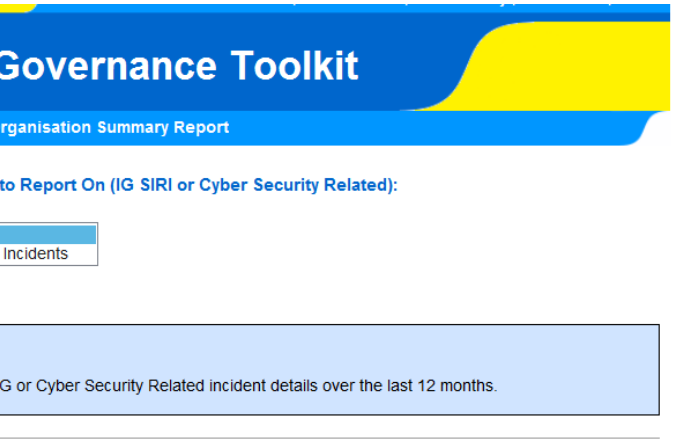
Previous Changes:

Date	By	Reason for Change	
23/10/2013 13:54:29	Lucy Lucas (ACUTEST)	testing closure	Show Changes
23/10/2013 12:04:29	Vanessa Kaliapermall (ACUTEST)	Test	Show Changes
21/10/2013 09:33:05	Lucy Lucas (ACUTEST)	test	Show Changes
17/10/2013 09:32:42	Lucy Lucas (ACUTEST)	testing edit of closed incident	Show Changes
16/10/2013 15:32:21	Lucy Lucas (ACUTEST)	test	Show Changes
16/10/2013 15:26:49	Lucy Lucas (ACUTEST)	Initial creation of incident	

4. The screen will refresh and the incident will appear now with an 'open' status.

3 How to Generate Reports

A. Incident Organisation Summary Report



Governance Toolkit

rganisation Summary Report

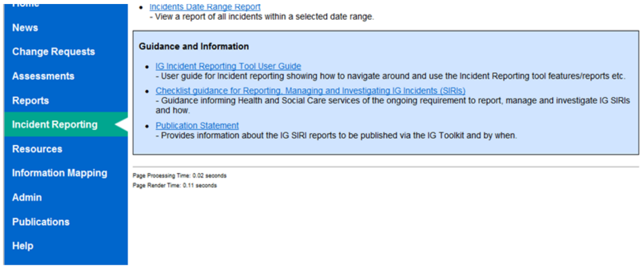
to Report On (IG SIRI or Cyber Security Related):

Incidents

G or Cyber Security Related incident details over the last 12 months.

Report

e page is the Incident Organisation Summary Report– see



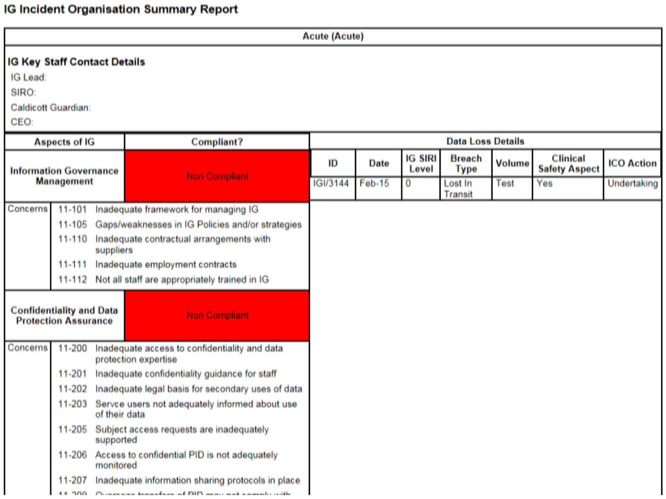
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

- IG Incident Reporting Tool User Guide
  - User guide for Incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

1. On clicking on the 'Incident Organisation Summary Report' link the following screen appears. You should choose which type of incident you wish to report on – IG SIRI or Cyber SIRI then click on link 'Show report'



IG Incident Organisation Summary Report

Acute (Acute)

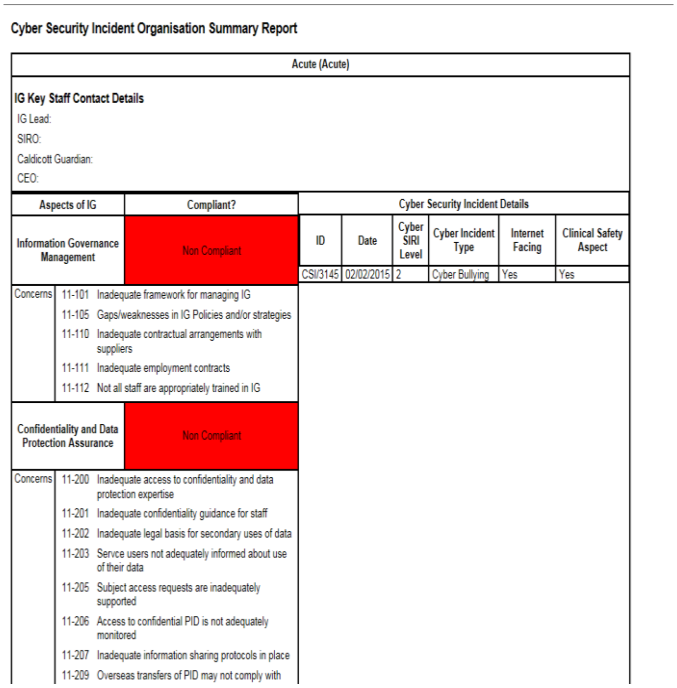
IG Key Staff Contact Details
IG Lead:
SIRO:
Caldicott Guardian:
CEO:

Aspects of IG		Compliant?
Information Governance Management		Non Compliant
Concerns	11-101 Inadequate framework for managing IG 11-105 Gaps/weaknesses in IG Policies and/or strategies 11-110 Inadequate contractual arrangements with suppliers 11-111 Inadequate employment contracts 11-112 Not all staff are appropriately trained in IG	
Confidentiality and Data Protection Assurance		Non Compliant
Concerns	11-200 Inadequate access to confidentiality and data protection expertise 11-201 Inadequate confidentiality guidance for staff 11-202 Inadequate legal basis for secondary uses of data 11-203 Servce users not adequately informed about use of their data 11-205 Subject access requests are inadequately supported 11-206 Access to confidential PID is not adequately monitored 11-207 Inadequate information sharing protocols in place 11-208 Overseas transfers of PID may not comply with	

Data Loss Details

ID	Date	IG SIRI Level	Breach Type	Volume	Clinical Safety Aspect	ICO Action
IGI/3144	Feb-15	0	Lost In Transit	Test	Yes	Undertaking

2. This presents a report (exportable in Word format) which could be used to inform senior management, Boards or interested Committees of any incidents which have been recorded in the last 12 months and an overview of the organisation's latest published IG Toolkit performance. The report column headings will be slightly different between IG and Cyber SIRI reports. See an example of each to the left and below.



Cyber Security Incident Organisation Summary Report

Acute (Acute)

IG Key Staff Contact Details

IG Lead:

SIRO:

Caldicott Guardian:

CEO:

Aspects of IG	Compliant?
Information Governance Management	🟥 Non Compliant
Concerns	11-101 Inadequate framework for managing IG 11-105 Gaps/weaknesses in IG Policies and/or strategies 11-110 Inadequate contractual arrangements with suppliers 11-111 Inadequate employment contracts 11-112 Not all staff are appropriately trained in IG
Confidentiality and Data Protection Assurance	🟥 Non Compliant
Concerns	11-200 Inadequate access to confidentiality and data protection expertise 11-201 Inadequate confidentiality guidance for staff 11-202 Inadequate legal basis for secondary uses of data 11-203 Servce users not adequately informed about use of their data 11-205 Subject access requests are inadequately supported 11-206 Access to confidential PID is not adequately monitored 11-207 Inadequate information sharing protocols in place 11-209 Overseas transfers of PID may not comply with

Cyber Security Incident Details

ID	Date	Cyber SIRI Level	Cyber Incident Type	Internet Facing	Clinical Safety Aspect
CSI/3145	02/02/2015	2	Cyber Bullying	Yes	Yes

- The ‘**IG Delivery Notes about the Organisation**’ section at the bottom of the page is read only for Organisations as this is an area for HSCIC and DH to note any particularly important information about the organisation which may be relevant when monitoring performance. It is an optional field to be used by HSCIC colleagues only on behalf of the DH or ICO. If no notes are recorded against your organisation then this section will not appear.

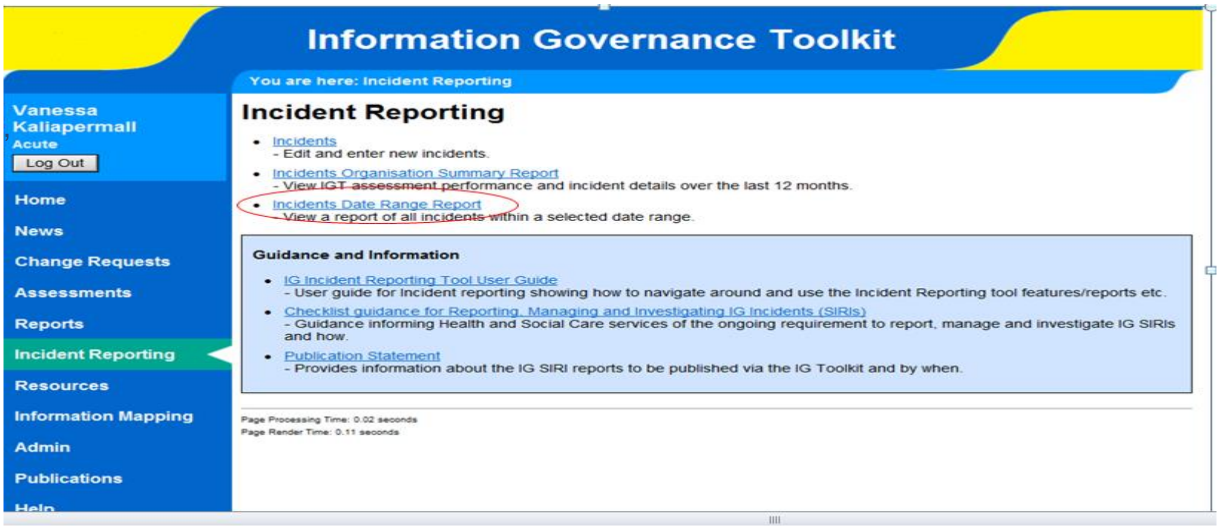
- The **‘IG Key Staff Contact Details’** are auto populated from your organisation’s latest entry against the IG Toolkit assessment summary screen (usually kept up to date by your local IGT Organisation Administrator) and are only there for reference if in case there is an major incident which requires the involvement and escalation to Senior Management within your organisation. When any changes are made to these details within the assessment summary screen the updates will be reflected in this report within a few minutes. If there are no details displayed under the IG Key Staff Contact Details section on this screen then you may wish to request your IG Toolkit Organisation Administrator populates the relevant section of the Assessment Summary screen or via the Admin Organisation Profile section of the Toolkit.

- This report is exportable to Word so that incidents can be escalated promptly or used as a report to senior management teams, Trust Boards etc.

B. Incident Date Range Report

The third link on the Incident Reporting page is the Incident Date Range Report– see screenshot below. The purpose of this report is to report on incidents by quarter or a specified date range.

1. **Click on 'Incident Date Range Report'**



Incident Reporting

- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

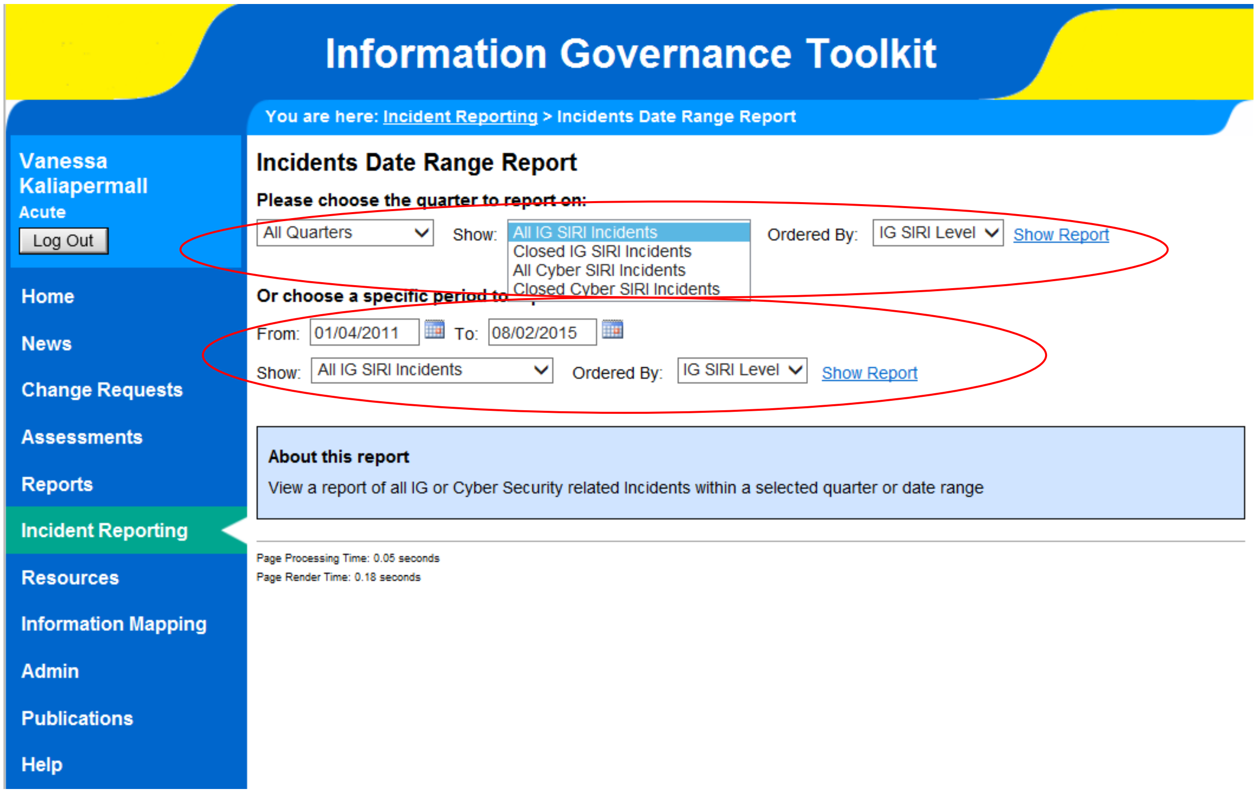
- IG Incident Reporting Tool User Guide
  - User guide for Incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

2. **To select the period of time the report is required to cover the user needs to choose either 'Please choose the quarter to report on:' or 'choose a specific period to report on.**

3. **Next select whether you would like to view a summary report of all incidents which have occurred during the period selected, or a summary report of all incidents which were closed during the period selected.**

4. **Once you have selected the period of time the report is required to cover and whether you would like to report on all incidents or closed incidents only (split by IG SIRIs or Cyber SIRIs), select the order that you would like the report to be displayed by (either by SIRI level or date the incident occurred/closed) click the 'Show Report' link to view the selected report.**



You are here: Incident Reporting > Incidents Date Range Report

Incidents Date Range Report

Please choose the quarter to report on:

All Quarters Show: All IG SIRI Incidents / Closed IG SIRI Incidents / All Cyber SIRI Incidents / Closed Cyber SIRI Incidents Ordered By: IG SIRI Level Show Report

Or choose a specific period to

From: 01/04/2011 To: 08/02/2015

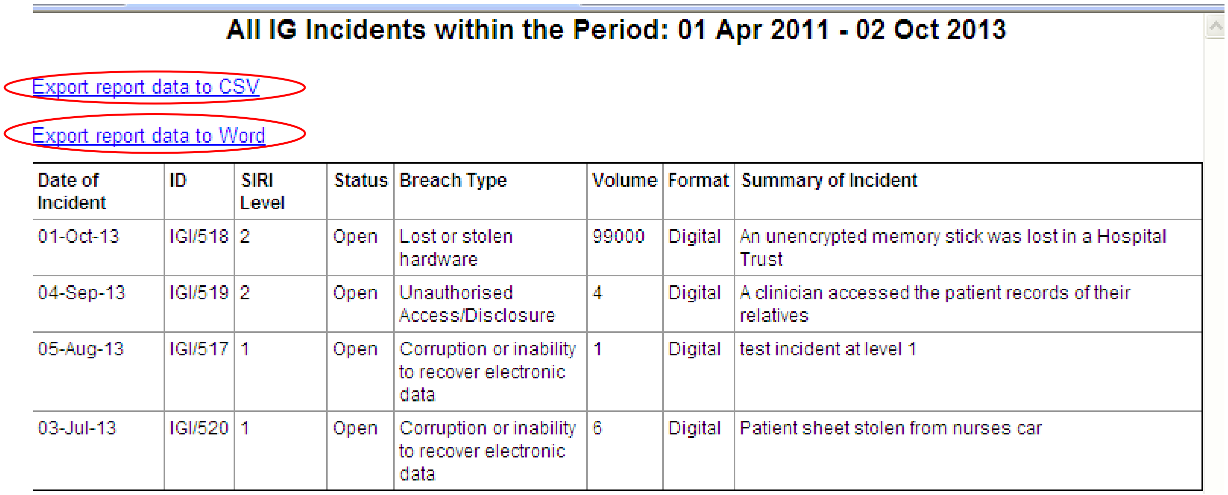
Show: All IG SIRI Incidents Ordered By: IG SIRI Level Show Report

About this report

View a report of all IG or Cyber Security related Incidents within a selected quarter or date range

Page Processing Time: 0.05 seconds
Page Render Time: 0.18 seconds

5. **Upon clicking 'Show Report' the following screen appears displaying your report (this screen may vary from the screenshot below depending on the parameters which you've selected for your report) and is exportable to CSV and Word formats as a pre-defined report. Please note that you may wish to format the CSV file (e.g. format headings in bold etc.) once saved to Excel as unfortunately the exportable CSV file will only allow limited formatting to be applied.**



All IG Incidents within the Period: 01 Apr 2011 - 02 Oct 2013

Export report data to CSV

Export report data to Word

Date of Incident	ID	SIRI Level	Status	Breach Type	Volume	Format	Summary of Incident
01-Oct-13	IGI/518	2	Open	Lost or stolen hardware	99000	Digital	An unencrypted memory stick was lost in a Hospital Trust
04-Sep-13	IGI/519	2	Open	Unauthorised Access/Disclosure	4	Digital	A clinician accessed the patient records of their relatives
05-Aug-13	IGI/517	1	Open	Corruption or inability to recover electronic data	1	Digital	test incident at level 1
03-Jul-13	IGI/520	1	Open	Corruption or inability to recover electronic data	6	Digital	Patient sheet stolen from nurses car

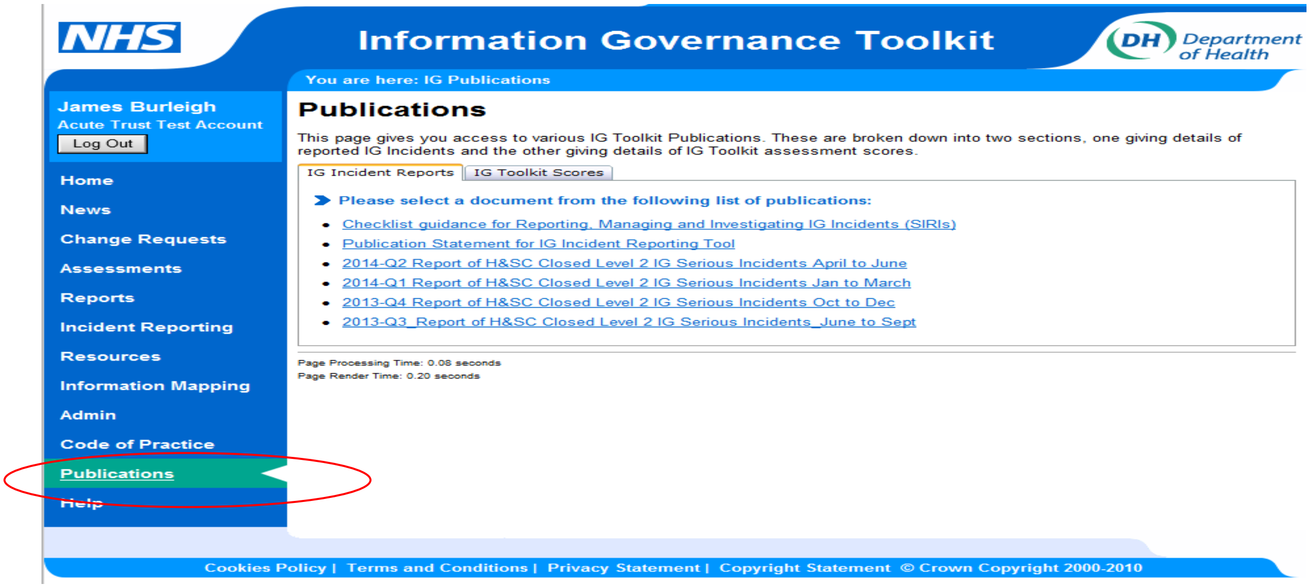
Closed Incident Reports

******Please note that all IG incidents which have occurred since 1st June 2013 (date this tool was launched to health and social care) and are now closed will appear in quarterly reports published on the IG Toolkit Publications tab available from the main left side menu. Therefore, it is advisable that Organisations check all closed incidents for completeness and accuracy before publication period. The quarters are January to March***

(Q1) through to October to December (Q4).A reminder note will be posted 6 weeks in advance of the quarter end date on the 'At a glance' page when you log into the IG Toolkit.

This does NOT INCLUDE CYBER SIRIs as for security purposes Cyber SIRIs will not be published. ***

Previous level 2 quarterly reports are published in the 'Publications' section of the IG Toolkit.



You are here: IG Publications

Publications

This page gives you access to various IG Toolkit Publications. These are broken down into two sections, one giving details of reported IG Incidents and the other giving details of IG Toolkit assessment scores.

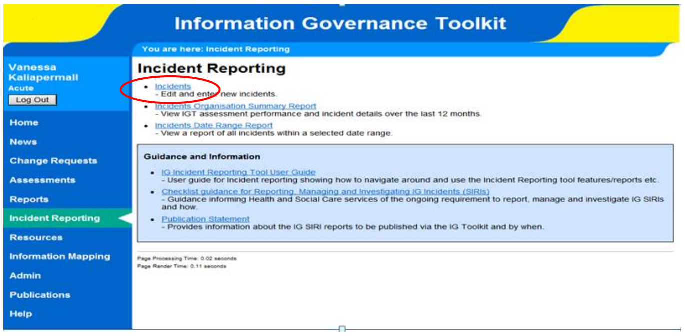
Please select a document from the following list of publications:

- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
- Publication Statement for IG Incident Reporting Tool
- 2014-Q2 Report of H&SC Closed Level 2 IG Serious Incidents April to June
- 2014-Q1 Report of H&SC Closed Level 2 IG Serious Incidents Jan to March
- 2013-Q4 Report of H&SC Closed Level 2 IG Serious Incidents Oct to Dec
- 2013-Q3_Report of H&SC Closed Level 2 IG Serious Incidents_June to Sept

Page Processing Time: 0.08 seconds
Page Render Time: 0.20 seconds

C. Database Search / Report

A search facility which you can use to run a search and then extract the results to a report if required is available on the 'Incidents'. The search will only search information held against your own organisation.



You are here: Incident Reporting

Incident Reporting

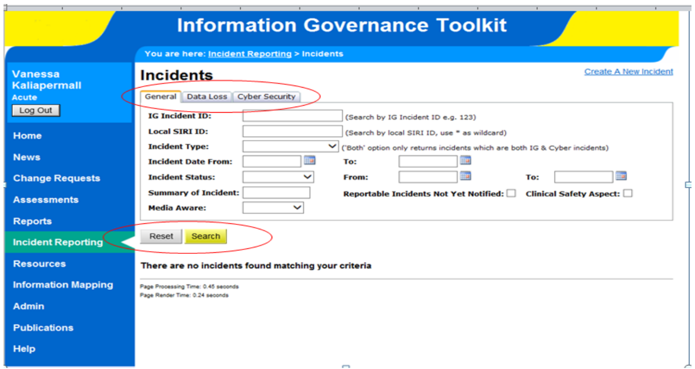
- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

- IG Incident Reporting Tool User Guide
  - User guide for incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

1. Go to 'Incidents' from the Incident Reporting home page.



You are here: Incident Reporting > Incidents

Incidents

Create A New Incident

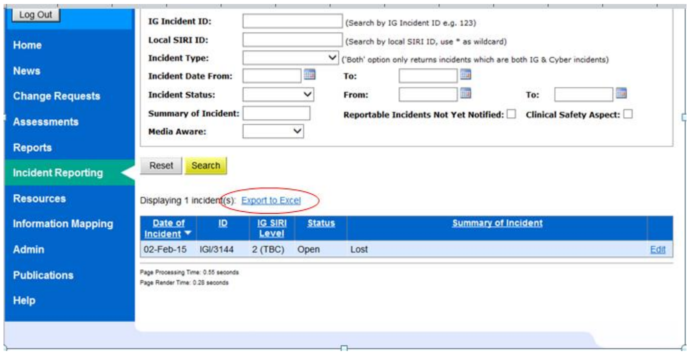
IG Incident ID: (Search by IG Incident ID e.g. 123)
Local SIRI ID: (Search by local SIRI ID, use * as wildcard)
Incident Type: ('Both' option only returns incidents which are both IG & Cyber incidents)
Incident Date From: To:
Incident Status: From: To:
Summary of Incident: Reportable Incidents Not Yet Notified: □ Clinical Safety Aspect: □
Media Aware:

There are no incidents found matching your criteria

Page Processing Time: 0.45 seconds
Page Render Time: 0.24 seconds

2. Complete the relevant fields of information you would like to perform a search based upon under the 'General' tab at the top of the screen. The 'Data Loss' (Data Breach) tab allows you to search by data fields relevant to IG SIRIs and the 'Cyber

Security' tab allows you to search by data fields relevant to Cyber SIRIs. Once you have set the search criteria click the 'Search' button to retrieve your results. Use the 'Reset' option to clear the search and start search selection again.



IG Incident ID: (Search by IG Incident ID e.g. 123)
Local SIRI ID: (Search by local SIRI ID, use * as wildcard)
Incident Type: ('Both' option only returns incidents which are both IG & Cyber incidents)
Incident Date From: To:
Incident Status: From: To:
Summary of Incident: Reportable Incidents Not Yet Notified: □ Clinical Safety Aspect: □
Media Aware:

Displaying 1 incident(s): Export to Excel

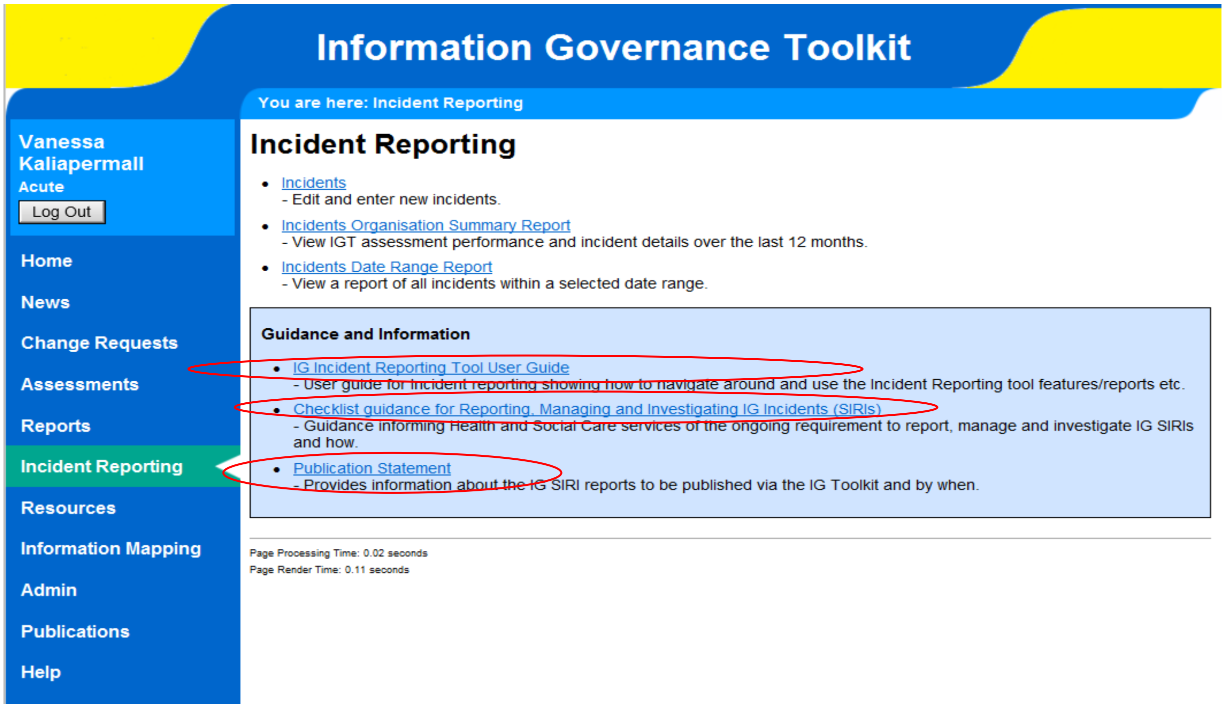
Date of Incident ▾	ID	IG SIRI Level	Status	Summary of Incident	
02-Feb-15	IGI/3144	2 (TBC)	Open	Lost	Edit

Page Processing Time: 0.55 seconds
Page Render Time: 0.28 seconds

3. The results of the search will be displayed in the box at the bottom of the page. You can then click the 'Export to Excel' link if you wish to export these into a spreadsheet format. Pivot tables in Excel can be used to convert the data into charts, graphs and statistics.

4 Where to go for help

- Guidance materials already described in this User Guide can be found on the Incident Reporting landing page when you click on Incident Reporting tab on left side menu when logged in. See screen shot below.
- If Users have any queries regarding this tool they should submit via the IG Toolkit helpdesk service by going to the 'Help' section and completing the online form under 'Contact us'. Select the appropriate category 'Incident Reporting Tool' under the 'Subject' field to ensure your query goes to the correct team for a response.



Incident Reporting

- Incidents
  - Edit and enter new incidents.
- Incidents Organisation Summary Report
  - View IGT assessment performance and incident details over the last 12 months.
- Incidents Date Range Report
  - View a report of all incidents within a selected date range.

Guidance and Information

- IG Incident Reporting Tool User Guide
  - User guide for incident reporting showing how to navigate around and use the Incident Reporting tool features/reports etc.
- Checklist guidance for Reporting, Managing and Investigating IG Incidents (SIRIs)
  - Guidance informing Health and Social Care services of the ongoing requirement to report, manage and investigate IG SIRIs and how.
- Publication Statement
  - Provides information about the IG SIRI reports to be published via the IG Toolkit and by when.

Page Processing Time: 0.02 seconds
Page Render Time: 0.11 seconds

Annex A Cyber SIRI and IG SIRI fields

The following map shows which fields are Cyber SIRI specific and which are IG SIRI specific.

Section/Fields	Value	Mandatory	Cyber	IG
Incident Subject Details (or Pop up box)			✓	✓
Cyber Security SIRI	Yes/No	✓	✓	✓
IG SIRI	Yes/No	✓	✓	✓
Clinical Safety Aspect	Checked indicates the incident has an impact on patient safety or provision of clinical care. Details of the clinical safety issue must be recorded on your dedicated local incident management systems and not within the IG Incident Reporting Tool. Only record details of the incident which are non-clinical in this tool (e.g. about the data loss). The local SIRI ID field should be used to record the identifier for the local system so that the reports can be linked/tracked if required.	✓	✓	✓
National System(s) or Network Affected	Whether this incident impinges upon a national system such as Spine 2, NHS Mail or a national network such as N3.	✓	✓	
Details of System(s) or Network Affected	Free Text		✓	
Organisation details			✓	✓
Code	Taken from login		✓	✓

Name	Taken from login		✓	✓
Type	Taken from login		✓	✓
Role	Taken from login		✓	✓
General Details			✓	✓
Status	Open/Closed/Withdrawn/Duplicate	✓	✓	✓
Cyber Reporter	Internal Staff / Technical Exterior People / Technical / Member of the Public / Third Party Contractors / Other	✓	✓	✓
Date of Incident:	Date	✓	✓	✓
Time of Cyber Incident	Time	✓	✓	
End date of Cyber incident	Date	✓	✓	
End time of Cyber incident	Time	✓	✓	
Duration of Cyber incident	From time of incident to a) current system clock or b) end time	✓	✓	
Local SIRI ID	The incident number or name identifier as displayed on the organisation's local incident management tool e.g. STEIS or equivalent. If there is no local SIRI ID then enter as 'none'**.**			
Related Incidents Recorded on IGT or Local System ID Number	This is the incident reference number for a related (but not the same) SIRI or Cyber incident either within this tool or a local system.			
Breach Type	Corruption or inability to recover electronic data, Disclosed in error, Lost in Transit, Lost or Stolen Hardware, Lost or Stolen	✓		✓

	Paperwork, Technical Security failing (including hacking), Unauthorised Access/Disclosure, Uploaded to website in error, Other.			
Cyber Incident Type	Hacking, DOS, Phishing Mails, Social Media Disclosures, Web site defacement, Malicious internal damage, spoof website, cyber bullying, other (please specify	✓	✓	
Cyber Incident Type details	Free text		✓	
How identified	Anti-Malware, Audit, External Notification, Firewall, Intrusion Detection System, System Logs, Other	✓	✓	
Summary of incident	This section should provide a brief, factual and concise description of what happened. This may be displayed in high level reports and may be made available in the public domain therefore this section must not include any personal/sensitive or commercially sensitive information	✓	✓	✓
Detail of Incident	Further detail in addition to the incident summary should be documented e.g.	✓	✓	✓

	detail on when the incident occurred , the types of records lost, information (e.g. Person Identifiable data items) contained within it, security measures in place or not, how it occurred, why and under what circumstances. What are the risks etc.			
Location(s) of Cyber Incident	For a SIRI incident this would generally be the physical location however when the breach is located in cyberspace this may be more problematic. If the location is undeterminable enter the location affected	✓	✓	
Internet Facing service?	Whether the service is internet facing or utilises an internet channel. you can have a service that utilises internet channel but the service itself is not internet facing - such as a file transfer service	✓	✓	
Severity Details			✓	✓
IG SIRI level	Level 0, 1 or 2			✓
Scale of the incident (Number of users or individuals affected)	As current	✓	✓	✓
Sensitivity factors	List of Medium and High Factors	✓		✓
Impact of Incident	Confidentiality /	✓	✓	

	Integrity / Availability / Clinical / Financial / Administrative / Reputational / Personal harm or distress / Environmental			
Cyber SIRI Level	Level 0, 1 or 2		✓	
Cyber Baseline Scale	The scale of the incident ranging from no impact on services, false alarm, individual or team/department affected or multiple departments or entire organisation. If unsure of which one of two levels please initially selected the higher one	✓	✓	
Cyber Sensitivity Factors	Aware that other organisations have been affected , Confidential information release (non-personal) or 100+ PCD Records, Critical business system unavailable for over 24 hours**,** Likely to attract media interest, Multiple attacks detected and blocked over a period of 1 month, Repeat Incident (previous incident within last 3 months?), Require advice on additional controls to put in place to reduce reoccurrence		✓	
Notified to Trusted National Bodies	Yes or no			

Data Details				✓
Data	Free Text	✓		✓
Format	Paper/Digital/Other			✓
Volume	Free Text	✓		✓
Encrypted	Yes/No/Password Protected only/Not Known/Not applicable			✓
Post Incident Details			✓	✓
Media Aware	Yes/No/Not Known etc.		✓	✓
Media Notes	Free Text		✓	✓
Data Subjects or Users Informed	Yes/No/Not Known/Not Required/Planned		✓	✓
Police informed	Yes/No/Not Known/Not Required/Planned		✓	✓
Actions taken	Free text		✓	✓
Root Cause Analysis	Drop down and or Free text Drop down values patching level, Firewall rules, Antivirus/malware coverage, external attack, internal attack , other (Please specify in RCA comments field)		✓	
RCA Comments	Free Text		✓	
Lessons learned	Free text		✓	✓
ICO Information				✓
ICO Informed	Populated when Level 2 is notified to the ICO via the tool			✓
ICO Action	Enforcement Notice/Undertaking /Monetary Penalty etc.			✓
ICO Action Date	Date			✓

Appendix A Autoclosure feature for Closing SIRI and Cybersecurity Incidents

The auto closure feature will automatically close incidents where no updates to an ‘open’ record have been undertaken within the last 90 days. Relevant incident reporting users will be notified by email 10 days in advance of planned auto closure and within 24 hours after closure.

The emails will be sent to all of the following persons:
a. The person that created the incident record.
b. The person that last updated the record
c. All organisation administrators who also are Incident Reporting users ; (if not already one of the persons specified under a. or b.)

This functionality will help to ensure records are kept up to date or closed within a reasonable time frame.

It should be noted that any incident that has been ‘auto closed’ can be re-opened at any time. Further instructions can be found in the incident reporting user guide available on the ‘Help’ page - Consideration should also be given to the quality, accuracy and appropriateness of level 2 closed incident reports and the commitment HSCIC has to publication of information as specified within the IG Toolkit Incident Reporting Publication Statement found on the IG Toolkit ‘Publication’ page.

User email notifications

Dear Colleague,
This is an automatic notification to inform you that the following incident(s) have not been updated for 80 days or more.

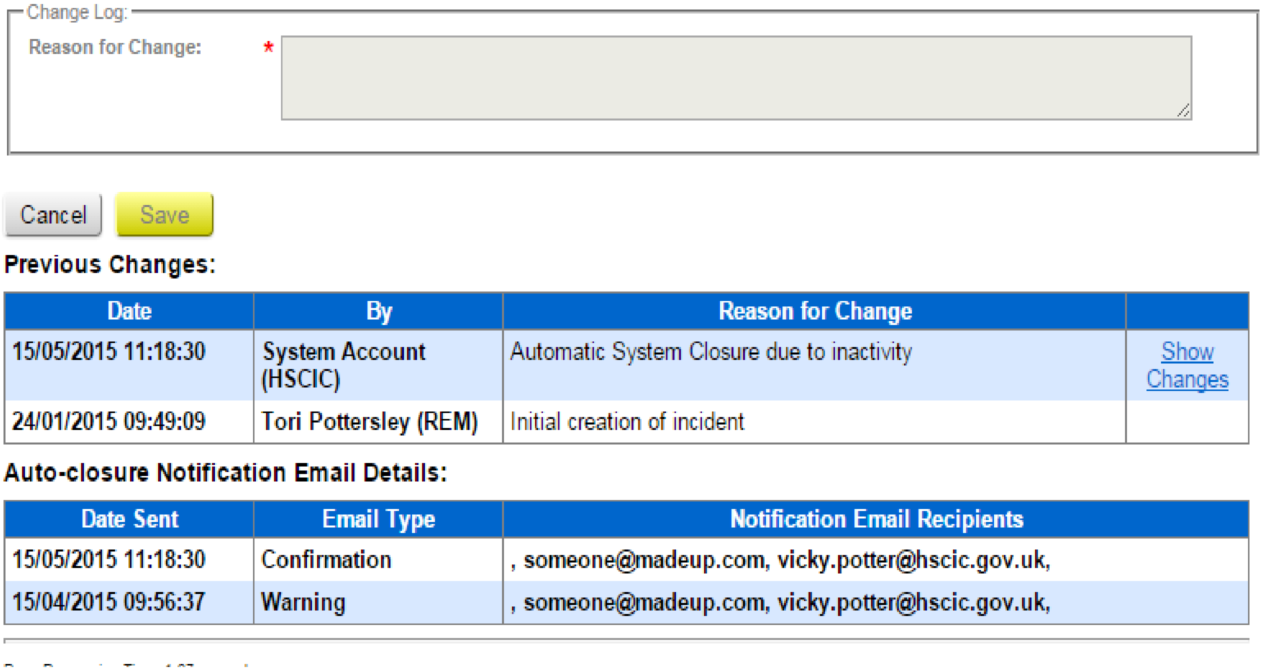
IGI/xxxxx; IGCSI/xxxx; CSI/xxxx; IGCSI/xxxx.

If you would like the incident(s) to remain open, you will need to update the incident(s) before [date].

If no update is made the incident(s) will automatically be closed 10 days after this email was sent. You will be sent a confirmation e-mail at the time of Closure.

Kind Regards

Information Governance Toolkit
Incident Reporting Tool



Change Log:

Reason for Change: *

Previous Changes:

Date	By	Reason for Change	
15/05/2015 11:18:30	System Account (HSCIC)	Automatic System Closure due to inactivity	Show Changes
24/01/2015 09:49:09	Tori Pottersley (REM)	Initial creation of incident	

Auto-closure Notification Email Details:

Date Sent	Email Type	Notification Email Recipients
15/05/2015 11:18:30	Confirmation	, someone@madeup.com, vicky.potter@hscic.gov.uk,
15/04/2015 09:56:37	Warning	, someone@madeup.com, vicky.potter@hscic.gov.uk,